IODM / 001

Interoperabilni dostopni medij

Tehnična specifikacija dostopnega medija

Različica: 0.4 · delovni osnutek
Datum: 25. november 2026
Spletno mesto: iodm.si

1. Predmet in področje uporabe

IODM (Interoperabilni dostopni medij) določa profil brezstičnih medijev (kartic, obeskov, …) za fizično kontrolo dostopa. Namen standarda je omogočiti uporabo medijev različnih proizvajalcev z bralniki različnih proizvajalcev sistemov kontrole dostopa (SKD). Profil določa komunikacijo, obliko potrdila in dokaz posedovanja zasebnega ključa.

Beseda **MORA** označuje obvezno zahtevo, **NAJ** priporočilo in **LAHKO** dovoljeno možnost. Skladnost s tem osnutkom ne pomeni certificiranja ali skladnosti z vsemi zahtevami navedenih mednarodnih standardov.

2. Normativne osnove

- ISO/IEC 14443 (deli 1–4): brezstični vmesnik in prenos.
- ISO/IEC 7816-4: organizacija datotek, APDU in podatkovni objekti.
- ISO/IEC 9798-3: avtentikacija z asimetričnimi mehanizmi.
- ISO/IEC 8825-1: BER in DER.
- RFC 5280 in RFC 5480: potrdila X.509 in zapis javnih ključev ECC.
- FIPS 186-5, FIPS 180-4 in NIST SP 800-186: ECDSA, SHA-256 in P-256.

Profil APDU in podpisnega sporočila je zasnovan na mehanizmu MIFARE DUOX ISOInternalAuthenticate, vendar je podporo standarda mogoče implementirati tudi na drugih platformah (recimo JavaCard).

3. Arhitektura in podatkovni model

Medij hrani potrdilo izdajatelja in pripadajoči zasebni ključ. Bralnik preveri potrdilo, generira in pošlje izziv in preveri podpis. Sistem za kontrolo dostopa (SKD) nato odloči o pravici dostopa na podlagi identitete poverilnice in lokalne politike.

Objekt	Identifikator	Zahteva
DF IODM	F041434345535301	Izbira po imenu DF
EF.Certificate	0101	Javno branje, DER X.509
EF.CertificateChain	0102	Neobvezno; glej § 4
Ključ avtentikacije	00	P-256, neizvozljiv

Ime DF je začasni, zasebni identifikator za razvoj in pilotne izvedbe. Pred stabilno javno izdajo je treba potrditi njegovo dodelitev in enoličnost. Datotečni identifikatorji so zapisani v omrežnem vrstnem redu. Medij MORA podpirati osnovni logični kanal, kratke APDU in ISO/IEC 14443-4. Bralnik NE SME zahtevati lastniških ukazov za redno preverjanje.

4. Potrdila in zaupanje

EF.Certificate MORA vsebovati eno potrdilo X.509 v DER od odmika 0, brez predpone, največ 4096 oktetov. Morebitno polnilo MORA biti ničelno. Bralnik določi dolžino iz zunanjega DER SEQUENCE.

4.1 Normativni profil potrdila končnega subjekta

Potrdilo MORA izpolnjevati RFC 5280 in RFC 5480 ter naslednje dodatne omejitve. Algoritmi so zapisani z OID; parametri obeh podpisnih AlgorithmIdentifier MORAJO biti odsotni, identifikatorja pa enaka.

Polje	Normativna vrednost

version	v3 (INTEGER 2)
serialNumber	Pozitivno, enolično pri CA, največ 20 oktetov po RFC 5280; ne IODM-ID
signature, signatureAlgorithm	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
issuer	Neprazno DN neposrednega izdajateljskega CA
validity	notBefore, notAfter v UTC; kodiranje po RFC 5280
subject	Natanko en RDN z enim atributom serialNumber (2.5.4.5)
subjectPublicKeyInfo.algorithm	id-ecPublicKey (1.2.840.10045.2.1)
Parametri SPKI	namedCurve prime256v1 (1.2.840.10045.3.1.7)
subjectPublicKey	BIT STRING, 0 neuporabljenih bitov, 04 + X + Y (65 B)
issuerUniqueID / subjectUniqueID	Odsotna
signatureValue	DER ECDSA SEQUENCE (r,s), ne surovi 64 B podpis APDU

Javni ključ MORA biti veljavna točka P-256, ne točka v neskončnosti. Zasebni ključ MORA biti namenski za IODM, ustvarjen ali varno vnesen v medij in neizvozljiv. Izdajatelj MORA preveriti dokaz posedovanja pred izdajo.

4.2 Identifikator medija v subject DN

Atribut subject.serialNumber MORA biti ASN.1 PrintableString (tag 0x13), natanko 12 znakov iz množice 0–9, A–F, brez presledkov, ločil ali predpone. Prvi štirje znaki so 16-bitni IID izdajatelja, zadnjih osem 32-bitni MID medija; oba sta v šestnajstiškem zapisu, najpomembnejši oktet prvi. IID 0000 in FFFF ter MID 00000000 in FFFFFFFF so rezervirani. IODM-ID je trajen identifikator medija; serialNumber potrdila pa identificira posamezno izdajo potrdila in se ob obnovi spremeni. Identifikator se ne sme ponovno dodeliti drugemu mediju. Bralnik MORA preveriti ujemanje IID z vpisom potrjenega CA v registru IODM-005. Identifikator se uporabi šele po uspešnem preverjanju verige, preklica in izziva. UID radijskega vmesnika ni nadomestilo.

Primer: IID=0001, MID=00001234, IODM-ID=000100001234. DER celotnega subject Name:

```
30 17 31 15 30 13 06 03 55 04 05 13 0C
30 30 30 31 30 30 30 30 31 32 33 34
```

4.3 Razširitve končnega potrdila

Razširitev (OID)	Kritičnost in vsebina
basicConstraints (2.5.29.19)	Obvezna, kritična; CA=FALSE, pathLen odsoten
keyUsage (2.5.29.15)	Obvezna, kritična; samo digitalSignature
subjectKeyIdentifier (2.5.29.14)	Obvezna, nekritična; SHA-1 nad biti javnega ključa po RFC 5280, metoda 1 (ni podpisni algoritem)
authorityKeyIdentifier (2.5.29.35)	Obvezna, nekritična; keyIdentifier enak SKI neposrednega CA
cRLDistributionPoints (2.5.29.31)	Obvezna, nekritična; najmanj en HTTPS URI celotnega CRL

authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Neobvezna, nekritična; OCSP ali calssuers
extendedKeyUsage (2.5.29.37)	Odsotna v osnovnem profilu
subjectAltName (2.5.29.17)	Odsotna

Druge nekritične razširitve so dovoljene le, če ne vsebujejo osebnih podatkov ali nasprotujočih identitet; neznane kritične razširitve se zavrnejo. Podvojene razširitve niso dovoljene. IODM ne zahteva lastnega OID; profil se določi z registrom in temi pravili. Najdaljša veljavnost končnega potrdila je 10 let; ne sme presegati veljavnosti neposrednega CA.

4.4 Veriga in preklic

Neobvezni EF.CertificateChain vsebuje zaporedje DER vmesnih CA od neposrednega izdajatelja navzgor, brez korenskega potrdila, največ 8192 B; brez polnila. Register MORA zagotoviti vsa vmesna CA potrdila za odobrene poti. Bralniku zato v osnovnem profilu ni treba brati neobveznega EF 0102. Sidra zaupanja in pripadajoči IID se pridobijo po IODM-005, ne z medija. Profil CA določa IODM-004. Bralnik MORA preveriti pot po RFC 5280, veljavnost, omejitve CA, podpis, profil končnega potrdila, IID in lokalno politiko. CRL/OCSP se preverja kriptografsko, za vse ne-korenske certifikate na poti; če svežih podatkov ni, se dostop zavrne. Naslovi iz potrdil se obravnavajo kot nezaupanja vredni; pridobivanje je omejeno na odobrene vire. Obnovitev potrdila istega medija ohrani IODM-ID, nova izdaja ima novo serijsko številko potrdila. Ob zamenjavi fizičnega medija se dodeli nov MID in prekliče staro potrdilo.

5. Izmenjava APDU

Vsi primeri uporabljajo šestnajstiški zapis; presledki niso del prenosa. C-APDU označuje ukaz, R-APDU odgovor. Vzorčni izzivi so namenjeni razlagi in se NE SMEJO uporabljati v produkciji.

5.1 Izbira aplikacije in datoteke

Bralnik izbere DF po imenu in nato EF.Certificate po identifikatorju. FCI ni zahtevan.

```
C: 00 A4 04 0C 08 F0 41 43 43 45 53 53 01
R: 90 00
C: 00 A4 02 0C 02 01 01
R: 90 00
```

5.2 Branje potrdila

Bralnik uporablja READ BINARY z odmikom v P1/P2 (15 bitov). Zaradi različne obravnave Le=00 na karticah IODM uporablja izrecne neničelne dolžine največ 240 oktetov. Najprej prebere štiri oktete glave DER, določi celotno dolžino in nato bere manjkajoče podatke v kosih. Dolžina MORA biti minimalno kodirana v DER in omejena pred dodelitvijo pomnilnika. Pri potrdilu dolžine 361 oktetov:

```
C: 00 B0 00 00 04
R: 30 82 01 65 90 00
C: 00 B0 00 04 F0
R: [240 oktetov] 90 00
C: 00 B0 00 F4 75
R: [117 oktetov] 90 00
```

Bralnik združi le podatkovne dele odgovorov. Pri krajši glavi DER prvi štirje okteti že vključujejo začetek vsebine. Bralnik zavrne nepričakovano kratke podatke ali neveljaven DER. Razširjeni APDU niso obvezni.

5.3 Enostranska avtentikacija medija

Bralnik pošlje INTERNAL AUTHENTICATE (INS 88), P1=00, P2=00. Obvezni OptsA je celoten TLV 80 09, ki vsebuje ime DF in različico protokola 01. Zunanji TLV 7C vsebuje izziv bralnika RndA (81 10). Bralnik MORA za vsak poskus ustvariti nov, nepredvidljiv 16-okteten izziv s kriptografskim generatorjem.

```
C: 00 88 00 00 1F
   80 09 F0 41 43 43 45 53 53 01 01
   7C 12 81 10
   A1 B2 C3 D4 E5 F6 07 18
   29 3A 4B 5C 6D 7E 8F 90
   56
```

Medij ustvari neodvisen 16-okteten RndB in podpiše naslednje sporočilo z ECDSA P-256 in SHA-256:

```
M = F0 F0 || OptsA_TLV || RndB || RndA
S = ECDSA-SHA256(Priv, M)
```

Podpis je 64 oktetov: r in s, vsak po 32 oktetov, nepredznačeno, najpomembnejši oktet prvi, z začetnimi ničlami po potrebi. Podpis ni DER SEQUENCE. SHA-256 se uporabi natanko enkrat. V podpis se vključi celoten OptsA, pri nonce pa samo vrednosti brez oznak in dolžin.

```
R: 7C 54 81 10
   11 22 33 44 55 66 77 88
   99 AA BB CC DD EE FF 00
   82 40 [r: 32 oktetov] [s: 32 oktetov]
   90 00
```

Odgovor MORA imeti 86 podatkovnih oktetov in status 9000. Bralnik MORA preveriti strukturo, dolžine, vrstni red, podpis in povezavo z izzivom trenutnega poskusa. Neznani, podvojeni ali odvečni objekti se zavrnejo. Vrednosti r in s morata biti v območju [1,n−1], kjer je n red osnovne točke P-256. Bralnik MORA vedno poslati predpisani OptsA in ga vključiti v preverjanje podpisa. Medij LAHKO sprejme druge vrednosti OptsA, vendar jih MORA vključiti v podpis nespremenjene. Avtentikacija ne vzpostavlja varnega kanala.

6. Statusne besede in obravnava napak

SW	Pomen
9000	Uspeh
6700	Napačna dolžina ukaza
6982	Varnostni pogoj ni izpolnjen
6984 / 6985	Ključ ali pogoji uporabe neustrezni
6987 / 6988	Manjkajoč ali neveljaven podatkovni objekt
6A82	Aplikacija ali datoteka ne obstaja

6A86 / 6A88	Napačni parametri ali neznan ključ
6Cxx	Napačen Le
6D00 / 6E00	Ukaz ali razred ni podprt

Bralnik MORA ob napaki prekiniti poskus in ne sme odobriti dostopa. Transportna napaka dovoljuje nov poskus z novim izzivom. Pri 6Cxx lahko ponovno izvede branje s popravljeno dolžino; pri 61xx lahko uporabi GET RESPONSE, če ga medij zahteva, vendar osnovni profil ne zahteva njegove implementacije. Nepričakovane statusne besede se obravnavajo kot neuspeh.

7. Varnost in zasebnost

Podpis svežega izziva preprečuje preprosto ponovno predvajanje in uporabo kopiranega potrdila brez zasebnega ključa. Ne preprečuje posredovanja APDU v realnem času (relay). Za okolja z večjim tveganjem so potrebni dodatni mehanizmi, npr. preverjanje bližine ali druga neodvisna potrditev.

Potrdilo in identifikator sta javno berljiva, zato je medij lahko sledljiv. Izdajatelj NAJ uporablja psevdonimne identifikatorje in v potrdilo ne vključuje osebnih podatkov, ki niso potrebni. Protokol ne avtenticira bralnika in ne zagotavlja zaupnosti. Ključ avtentikacije NAJ bo namenjen izključno IODM. SKD MORA ločevati kriptografsko avtentikacijo od avtorizacije in dostop odobriti le ob veljavni politiki. Dnevniki NAJ hranijo najmanjši potreben obseg podatkov.

8. Implementacija in skladnost

Na MIFARE DUOX je treba ustvariti aplikacijo z ustreznim ISO DF imenom, javno berljivo datoteko StandardData (ISO EF 0101) in aplikacijskim ECC ključem 00, omogočenim za card-unilateral authentication prek NFC. Medij mora biti v neavtenticiranem stanju. Za IODM datoteko se uporabi neposreden DER zapis, ne tovarniška oblika Cert.PICC s predpono. DUOX Priv.PICC ni privzeto omogočen za ta mehanizem; tovarniško potrdilo ni nadomestilo za potrdilo poverilnice IODM. Pri Java Card ali drugi platformi se enaka semantika implementira v aplikaciji.

Formalno preverjanje skladnosti medija določa IODM-002, preverjanje bralnika pa IODM-003. Naslednja tabela povzema skupne varnostne cilje:

Preskus	Pričakovani rezultat
Veljavno potrdilo, svež izziv, pravilen podpis	Avtentikacija uspe
Ponovitev odgovora ob novem izzivu	Zavrnitev
Spremenjen RndB, OptsA ali podpis	Zavrnitev
Potrdilo z drugim javnim ključem	Zavrnitev
Nezaupanja vreden CA, potek ali preklic	Zavrnitev
Napačne dolžine ali podvojeni TLV	Zavrnitev

Veljavna poverilnica brez pravice dostopa	Zavrnitev dostopa

Ta izdaja je razvojni osnutek. Pred produkcijsko uporabo so potrebni medplatformni preskusi, formalni testni vektorji, pregled politike PKI in dokončna dodelitev identifikatorjev. Primeri APDU niso zajeti iz fizičnega medija.

9. Medproizvajalska interoperabilnost

9.1 Ločitev vlog

Proizvajalec medija, izdajatelj poverilnice, proizvajalec čitalnika in upravljavec sistema dostopa so neodvisne vloge. Izdajatelj LAHKO uporablja več platform medijev; upravljavec LAHKO združuje medije več izdajateljev in čitalnike več proizvajalcev. Skladnost se presoja na javnem vmesniku, ne na notranji izvedbi.

9.2 Obvezne zahteve

- Čitalnik MORA uporabiti isto zaporedje APDU ne glede na proizvajalca, ATR/ATS, UID ali ime izdajatelja. Odstopanja v transportu se obravnavajo na transportni plasti.
- Čitalnik NE SME zahtevati proizvajalčevega SDK, SAM, posebnih simetričnih ključev ali spletnega API izdajatelja za izvedbo osnovnega protokola.
- Dodajanje podprtega izdajatelja MORA biti možno s spremembo konfiguracije zaupanja in politike, brez spremembe protokola ali programske kode.
- Medij NE SME zahtevati predhodne registracije čitalnika, lastniške izbire aplikacije ali avtentikacije čitalnika za osnovni profil.
- Različne kartične platforme, vključno z namenskim IC in programirljivimi pametnimi karticami, so dopustne, če izpolnjujejo IODM-002. Mobilna emulacija je dopustna le ob izpolnitvi vseh zahtev, vključno z zaščito ključa.
- Čitalnik MORA razlikovati avtentikacijo od avtorizacije. Veljaven medij drugega izdajatelja ne pridobi samodejno pravice dostopa.
- Lastniške razširitve NE SMEJO spreminjati osnovnega zaporedja ali povzročiti, da bi čitalnik moral poznati proizvajalca. Neznane različice profila se zavrnejo brez prehoda na UID.

9.3 Življenjski cikel

Zamenjava čitalnika ne sme zahtevati ponovne izdaje medijev, če novi čitalnik podpira isti profil in politiko zaupanja. Zamenjava izdajatelja zahteva posodobitev zaupanja in po potrebi preslikavo identitet v SKD. Izdajatelj MORA dokumentirati način preklica, menjave CA in potrdil. Trditve o združljivosti veljajo samo za preskušene različice strojne in programske opreme.

10. Register potrjenih izdajateljev IODM

10.1 Namen in objava

Na iodm.si se predvidi javni register CA potrjenih izdajateljev. Register predstavlja seznam preverjenih izdajateljev, ne seznama oseb, ki imajo dovoljenje za dostop. Objava CA ne pomeni samodejnega zaupanja v katerem koli SKD. Upravljavec izrecno določi dovoljene izdajatelje in obseg uporabe.

Obvezna polja registra, vključno z IID, statusi in prstnimi odtisi potrdil, določa IODM-005. Profil registra je vezan na izdajo IODM-001/0.4. Podatki o preklicu posameznih potrdil so dostopni prek CRL/OCSP.

10.2 Sprejem izdajatelja

Upravljavec registra MORA pred vpisom preveriti identiteto in pooblastila izdajatelja, dokaz nadzora nad ključem CA (podpis svežega izziva ali enakovreden dokaz), verigo in omejitve CA, politiko izdaje, neizvozljivost ključev medijev, postopek preklica in odziv na incidente. Izdajatelj predloži veljavno poročilo IODM-002 za vsako priglašeno izvedbo medija. Zasebnih ključev se ne predloži. Odločitev, dokazi in obseg vpisa se evidentirajo; vpis se redno ponovno pregleda.

10.3 Distribucija in posodobitve

Pred produkcijsko uporabo MORA upravljavec registra objavljati podpisan manifest z monotonim zaporedjem izdaje, časom izdaje in izteka ter zgoščenimi vrednostmi vseh objavljenih potrdil. Oblika je JSON v UTF-8 in ločen podpis CMS SignedData nad natančnimi bajti datoteke; javni ključ podpisnika registra se varno namesti izven registra. HTTPS je dodatna zaščita, ne nadomestilo podpisa. Normativni profil CMS in shemo določa IODM-005.

Čitalnik ali njegov SKD MORA preveriti podpis, veljavnost, zaporedje (zaščita pred povrnitvijo stare različice), prstne odtise in lokalno politiko pred aktivacijo. Posodobitev MORA biti atomska. Neveljaven paket se zavrne; zadnji veljavni paket se sme uporabljati le do izteka in v skladu z lokalno politiko. Po izteku se dostop ne odobri na podlagi zastarelega zaupanja. Umaknjene in začasno ustavljene vpise je treba izključiti iz novih avtentikacij. Menjava CA se izvede z ločenima vpisoma potrdil znotraj istega IID in časovno omejenim prekrivanjem. Register ne nadomešča CRL/OCSP posameznih potrdil.

10.4 Status registra

V tej izdaji je register načrtovan; seznam je prazen, podpisni ključ in produkcijski postopek še nista vzpostavljena. Praznega razvojnega seznama ni dovoljeno uporabljati kot produkcijski vir zaupanja.